Communication Paths for Eleven Key Areas of SFA Security & Privacy

Area 1: Incident Response

- An enterprise-wide episodic communications method to respond immediately to IT security issues such as DDOS, destruction of data, and virus attacks.

Area 2: System Operations

- An enterprise-wide episodic and periodic communication method to convey system and application status to security managers, users, partners and customers. Includes messages about system downtimes, scheduled maintenance and any problems affecting daily use.

Area 3: Policy

- Develop communication paths to make sure all SFA security managers, users and partners know about existing, new, and changes to SFA IT security and privacy policy.

Area 4: Training

- SFA's complete security training plan that makes sure all employees, security managers and security professionals have the required and recommended knowledge to complete their jobs securely. Internal/Departmental training as well as outside training opportunities and conferences form the pool of resources in this SFA security area.

Area 5: Information Distribution

- Establish an effective and recognized communication channel stemming from the CSO office that reaches out to all SFA employees and security managers to distribute security and privacy information on a periodic and episodic basis. This involves relating internal SFA security and privacy developments and forwarding information from the security profession which benefits SFA security and privacy practitioners, such as news of external security incidents.

Communication Paths for Eleven Key Areas of SFA Security & Privacy

Area 6: Configuration Management

- How to establish the CSO office in the CM process so that security is integrated and standardized across all applications

Area 7: Procurement

- How to make sure the CSO office plays a part in the security aspects of the procurement cycle from requirements development to final acceptance of goods or services.

Area 8: Clearances and Access

- Identify the central office SFA uses for personnel clearances, and define the path a user and security manager must follow to obtain or terminate system access privileges.

Area 9: Certification and Accreditation (C & A)

- Describe the security manager communication lines that support the official validation of SFA systems and security procedures and relate the results back to management.

Area 10: Security Professionals Information Exchange

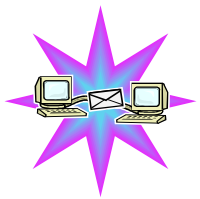
- Establish routine communication channels among SFA security managers that create forums in which SFA security issues can be discussed. Also establish the avenue by which results of these exchanges can be distributed.

Area 11: User Questions and Answers

- Design ways SFA users can get answers to their security question, “How do I…?” Make the user feel comfortable they can reach help.

Diagram Descriptions

Direct communications conducted in-person or by phone



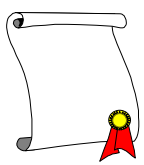
Email sent from one person to another or to a group of people

Telephone broadcast message left in every user's voice mail box

Information communicated in a meeting

Information communicated by a web page or FTP

Information communicated by a document



Information communicated as policy

Area 1: Incident Response – Internal Incidents

Purpose: To quickly exchange information systems incidents throughout SFA

Messages

- Timely information about the incident, indicating what happened, the implications, corrective actions, estimated time for systems to regain operability, and other systems potentially at risk

Responsibilities

- Systems personnel, help desks, and users must report incidents to SSO who in turn notifies the SM
- SM reports to the FM, as well as the CSO
- CSO notifies the CIO, COO, Partners and Customers as appropriate, and contacts other impacted FMs and SPAs who will notify SMs of the incident
- For incidents that require immediate dissemination to all SFA users, CSO notifies all SFA employees through blanket email and broadcast voicemail
- CIO contacts Public Affairs for cases with press interest and contacts the IG for cases requiring criminal investigation

Communication Methods

- Due to the need for timely and thorough communications, incidents will be identified either through face-to-face discussions or through telephone conversations

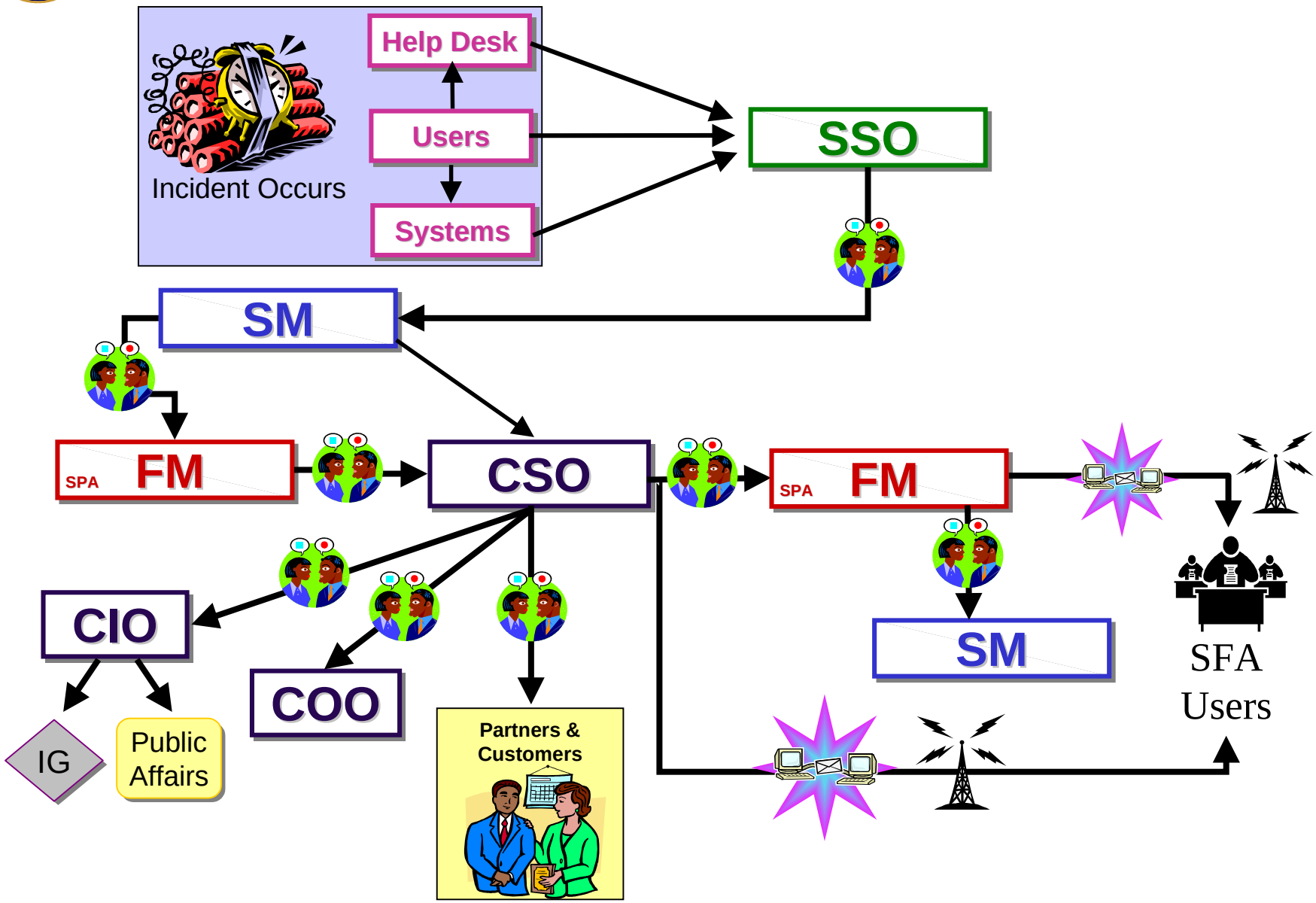
External Communications

- Communication outside of the security team may be necessary for certain incidents that impact external partners or customers, or attract media attention

Timeframe

- Notification of incidents must be communicated with the security team as quickly as possible after discovery; follow the chain-of-command for the notification process
- External communications must also be conducted in a timely manner to notify all parties affected

Area 1: Incident Response – Internal Incidents



Area 1: Incident Response – External Incidents

Purpose: To quickly report information system incidents from outside sources throughout SFA

Messages

- Timely information from CERT, CIRC or NIPC about incidents that happened outside SFA indicating what happened, the implications, and corrective actions

Responsibilities

- CERT reports incidents to CSO (as an addressee on their email list), and CSO surfs websites of NIPC and CIRC
- CSO then determines whether or not the incidents affect SFA
- For outside incidents that affect SFA, CSO will immediately disseminate information to all SFA users and affected Partners and Customers
- For outside incidents that do not affect SFA, CSO posts a notification on the Intranet for SFA users to read

Communication Methods

- Receive email notifications from CERT and surf websites of NIPC and CIRC
- Communication to SFA users about external incidents will be done via email, broadcast voicemail or the Intranet depending on the nature of the incidents and whether the incident has direct impact to SFA operations

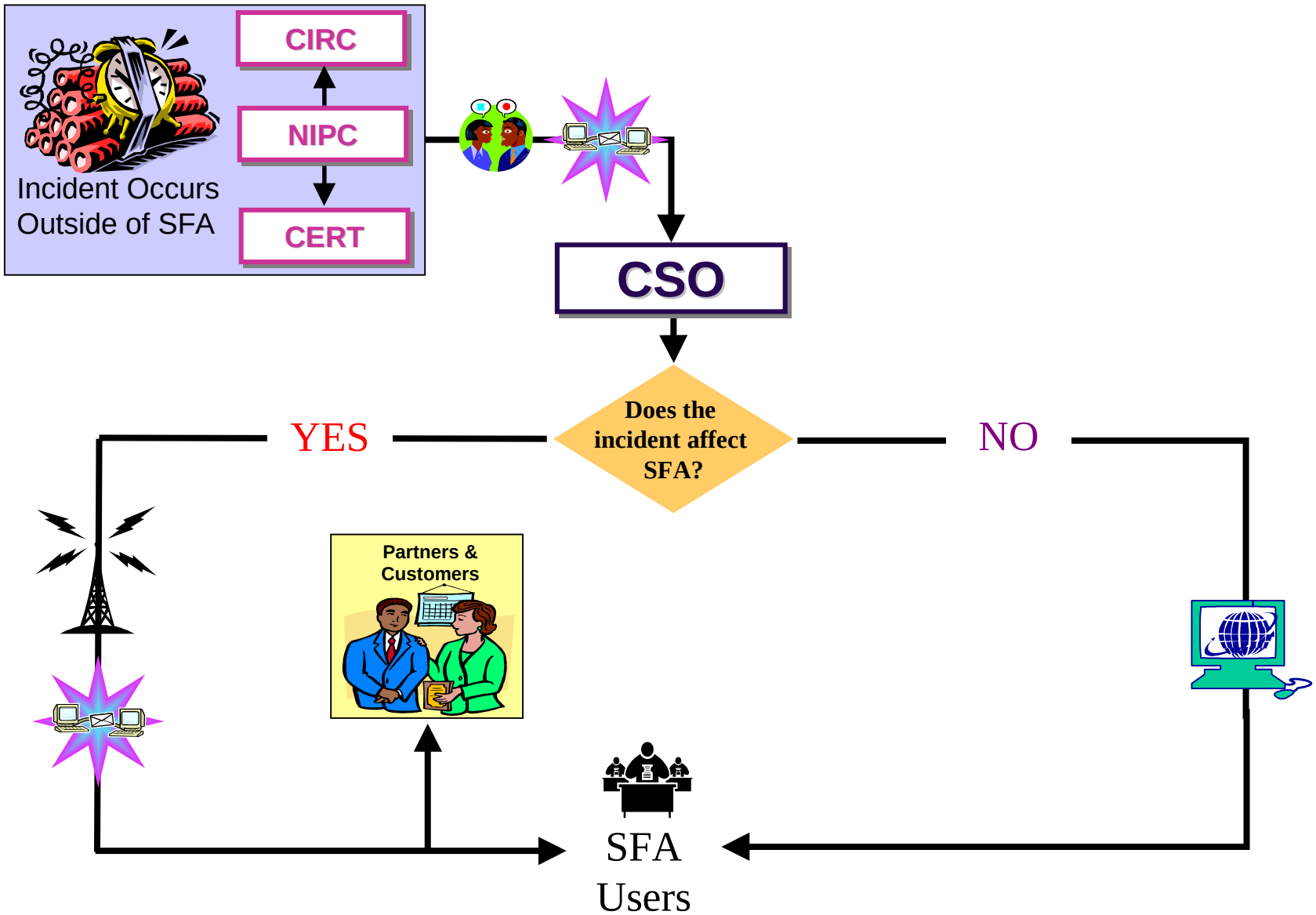
External Communications

- Between CERT, CIRC or NIPC and CSO
- Between SFA and partners and customers affected by the incidents

Timeframe

- For incidents that directly affect SFA, the CSO must inform SFA users as soon as possible
- For incidents that do not affect SFA, the CSO informs SFA users on an FYI-basis by posting notices on the Intranet

Area 1: Incident Response – External Incidents



Area 2: System Operations

Purpose: To disseminate information about SFA systems and applications status throughout SFA and to partners and customers

Messages

- Inform all participants of changes in the operating status of SFA systems or applications
- Convey change of system status, expected completion time and known impacts

Responsibilities

- Systems personnel, help desks and users must report status changes (planned and unplanned) to SMs
- SM reports the status change to FM
- FM seeks advice of the SPA as needed
- FM acknowledges the status change and directs the SM to communicate the outage to the rest of SFA, partners, customers and other organizations

Communication Methods

- Notifications take place via written memoranda, email or the web
- Maximum coverage of all SFA, partners, customers and outside organizations is desired

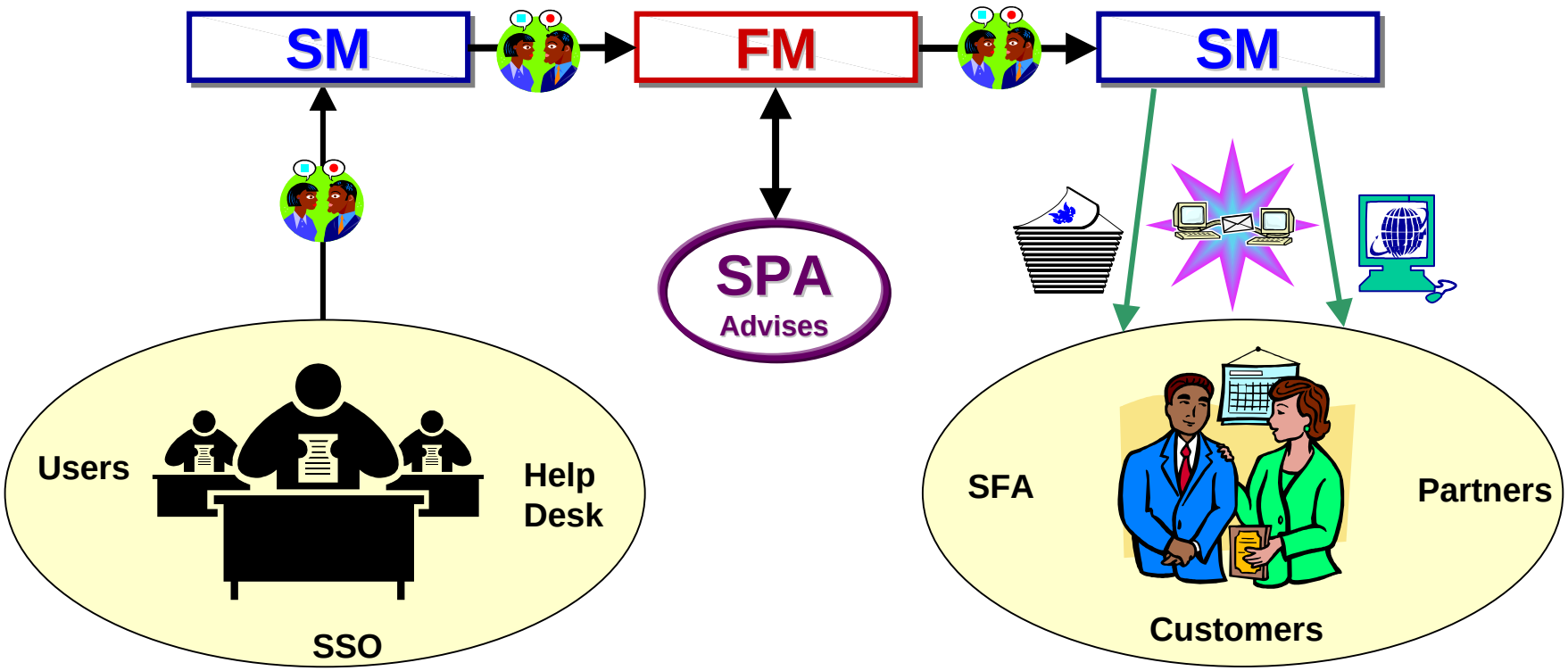
External Communications

- Share changes in system operations with effected partners, customers, or other organizations such as the Department of Education

Timeframe

- For non-scheduled changes in status, notify all impacted parties as soon as possible
- For planned changes in status, one week advance notification to the end users and impacted communities is desired

Area 2: System Operations



Area 3: Policy

Purpose: To disseminate security and privacy policy and policy updates throughout SFA, its partners, and customers; to provide a mechanism for the submission of recommended policy changes from every level of SFA

Messages

- Communications inform all participants of the most recent SFA security and privacy policy, emphasizing maximum coverage throughout SFA

Responsibilities

- New policy ideas and changes to existing policy are submitted to the Management Council by SPAs, FMs, CSO, SMs, and SFA users
- After the Management Council reviews and approves policy, it is forwarded to the CSO for dissemination to all SFA users, partners, and other organizations, as appropriate
- Security and privacy policies affecting SFA customers will be displayed on appropriate internet web pages

Communication Methods

- Notification of a new policy is communicated via email from the CSO
- Complete policy information is available on the intranet/extranet
- New policy or policy changes can be recommended by email or during working group sessions
- Security and privacy policies affecting customers are available via links on internet web pages

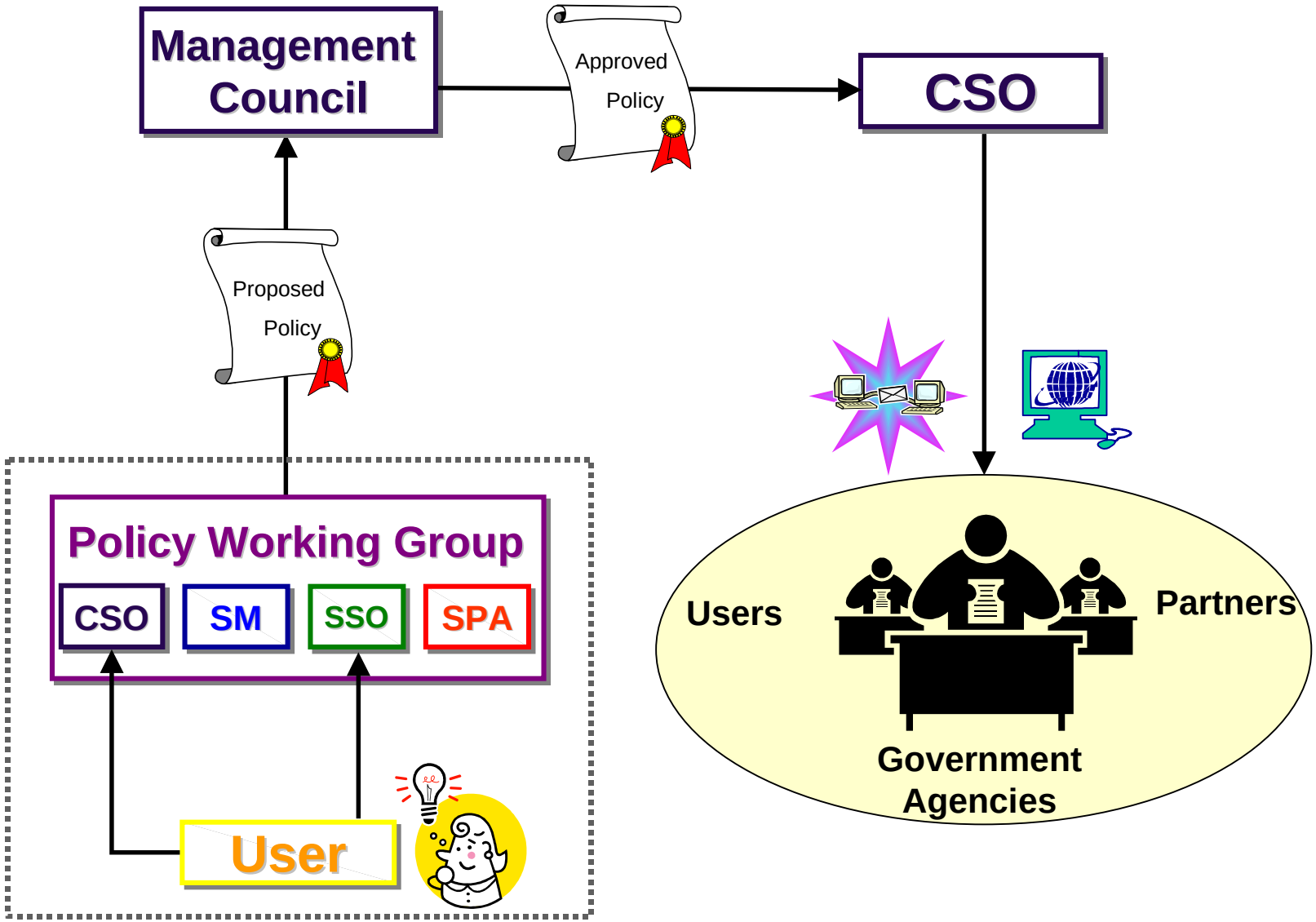
External Communications

- Communication with partners, customers and contractors will be done by FTP, email and internet

Timeframe

- New policy must be communicated to all SFA users, partners, and other organizations in a timely manner
- Policy should be distributed with adequate time for all parties to implement it

Area 3: Policy



Area 4: Training

Purpose: To exchange training requirements and opportunities throughout SFA and its partners and provide training to users and security professionals

Messages

- Inform security managers and users of required training (initial, annual, specialized) based on their roles
- Publicize training schedules and locations
- Determine requirements for specialized security training
- Hold training sessions

Responsibilities

- CSO staff identifies and schedules mandatory security awareness training for all SFA employees
- CSO staff coordinates with Department of Education training officials and SFA University and searches for outside training opportunities
- SMs and SSOs identify mandatory system security training and establish training schedules
- Training working group (CSO, SPAs, SSOs) confirm requirements, establish regimens and approve proposed curriculums

Communication Methods

- Training program, role requirements and schedules are posted on SFA intranet
- Training working group meets in-person to discuss training topics
- Email and website are used to make sure all SFA employees know when to attend training
- Specialized training courses are identified to security managers and systems personnel via email

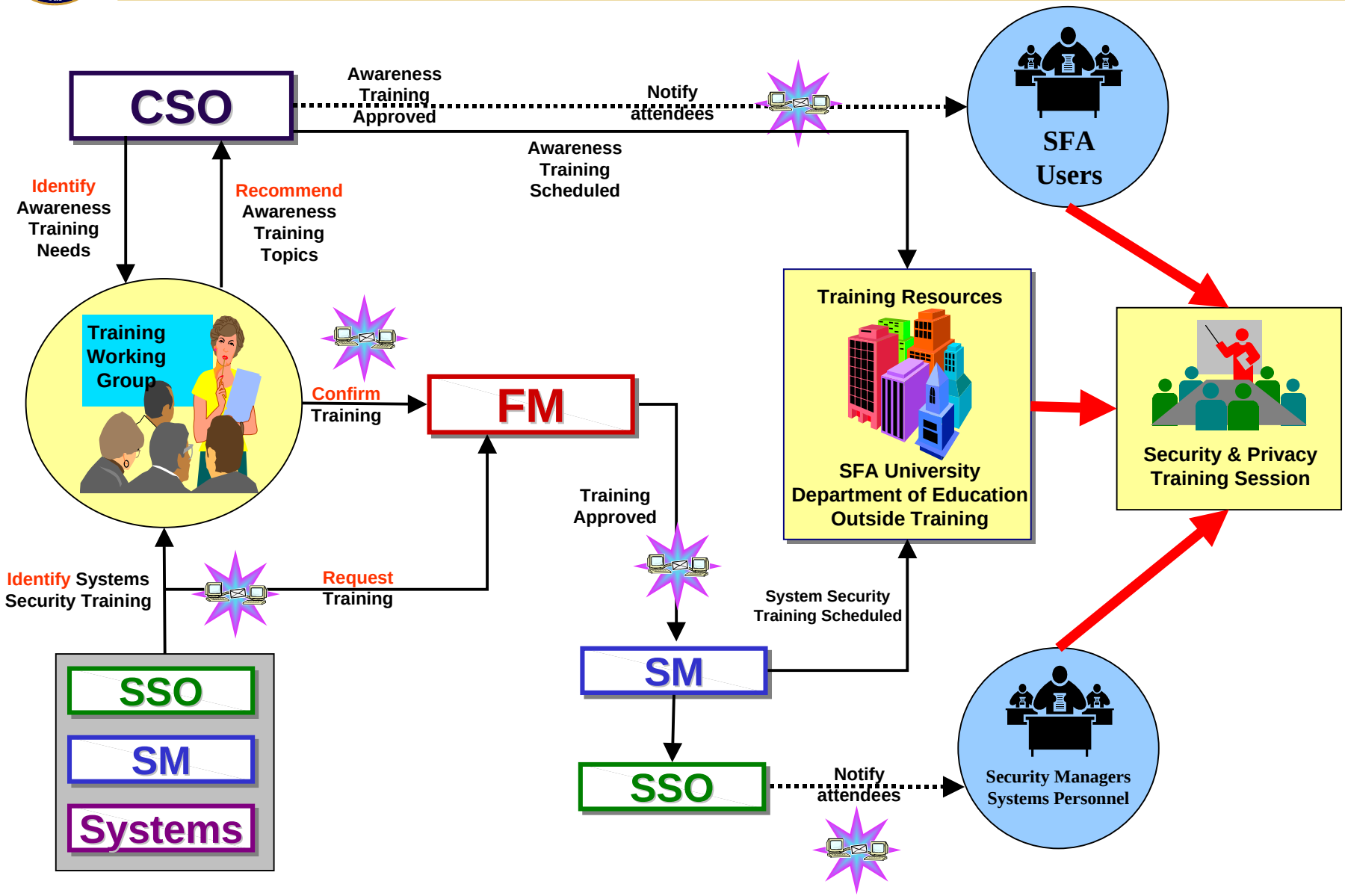
External Communications

- Inform external participants, partners and contractors of training, making materials available on-line when possible

Timeframe

- Meet mandatory initial (30-day) and annual security training requirements
- Notify those who need training in time for them to attend the required training

Area 4: Training



Area 5: Information Distribution

Purpose: To establish an effective and recognized communication channel from the CSO office that reaches out to all SFA employees and security managers to distribute security and privacy information on a periodic and episodic basis

Messages

- Relate internal SFA security and privacy developments and initiatives
- Announce periodic security and privacy events like clearance updates and password changes
- Pass on information from the security profession which benefits SFA security and privacy practitioners, such as news of outside security incidents
- Distribute security material related to systems in use by SFA, legislative or oversight activities that may impact SFA, or new technologies that may be adopted by SFA

Responsibilities

- CSO and his staff monitor current security events and state of security tools and technologies and distribute the information to SFA users and security managers based on content
- SPA distributes periodic information from the CSO staff to the FM, SM, SSO and users
- CSO staff distributes information needing immediate attention directly to all SFA employees

Communication Methods

- SFA Security & Privacy website acts as a central resource for SFA security and privacy information
- Periodic bulletins for SFA security managers and users distributed via email and posted on web site
- Email and phone calls expedite information requiring immediate distribution
- Existing staff meetings, management councils, etc., provide a vehicle for verbal distribution

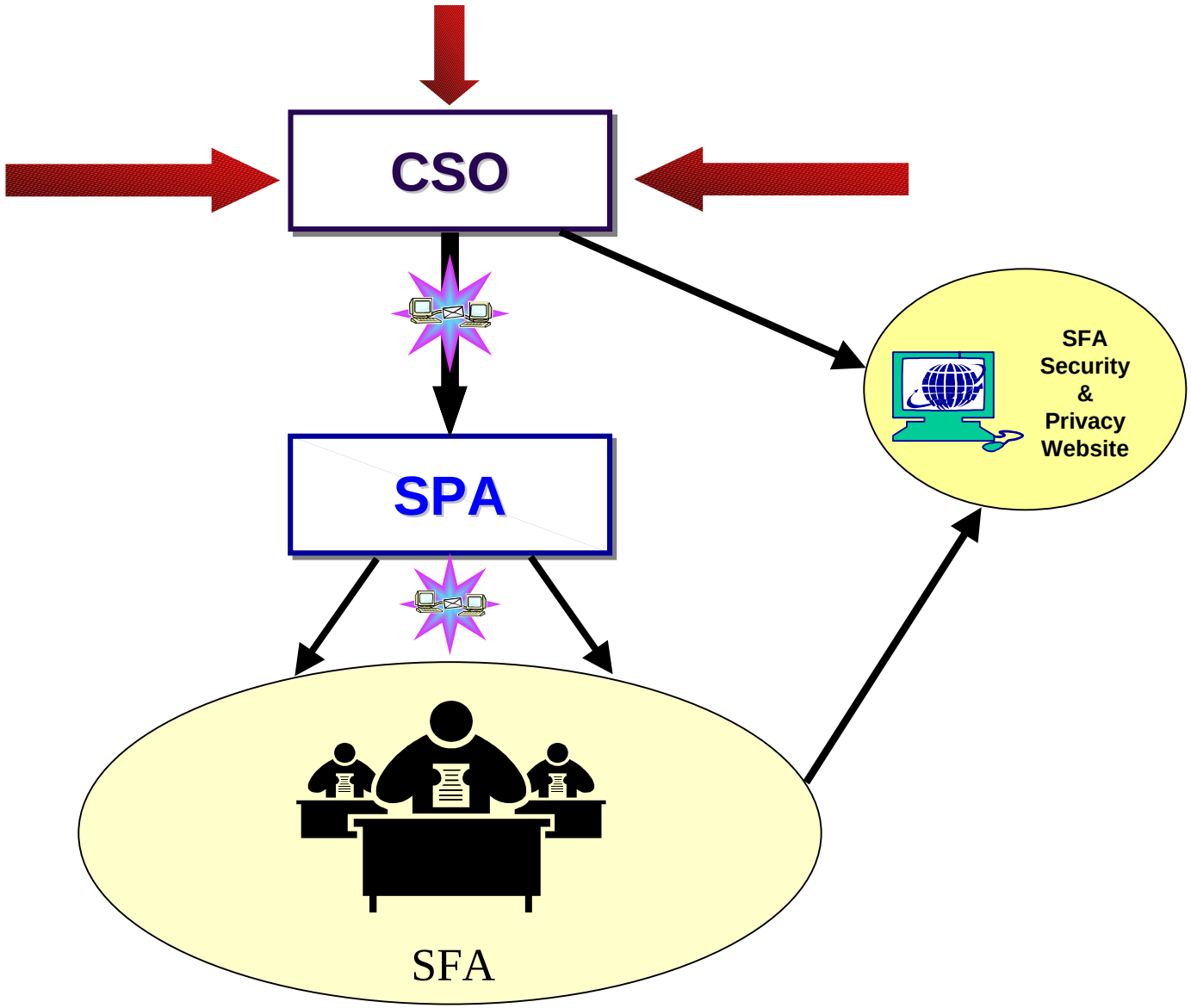
External Communications

- Security practitioners at schools and partners should be included in the appropriate distribution lists

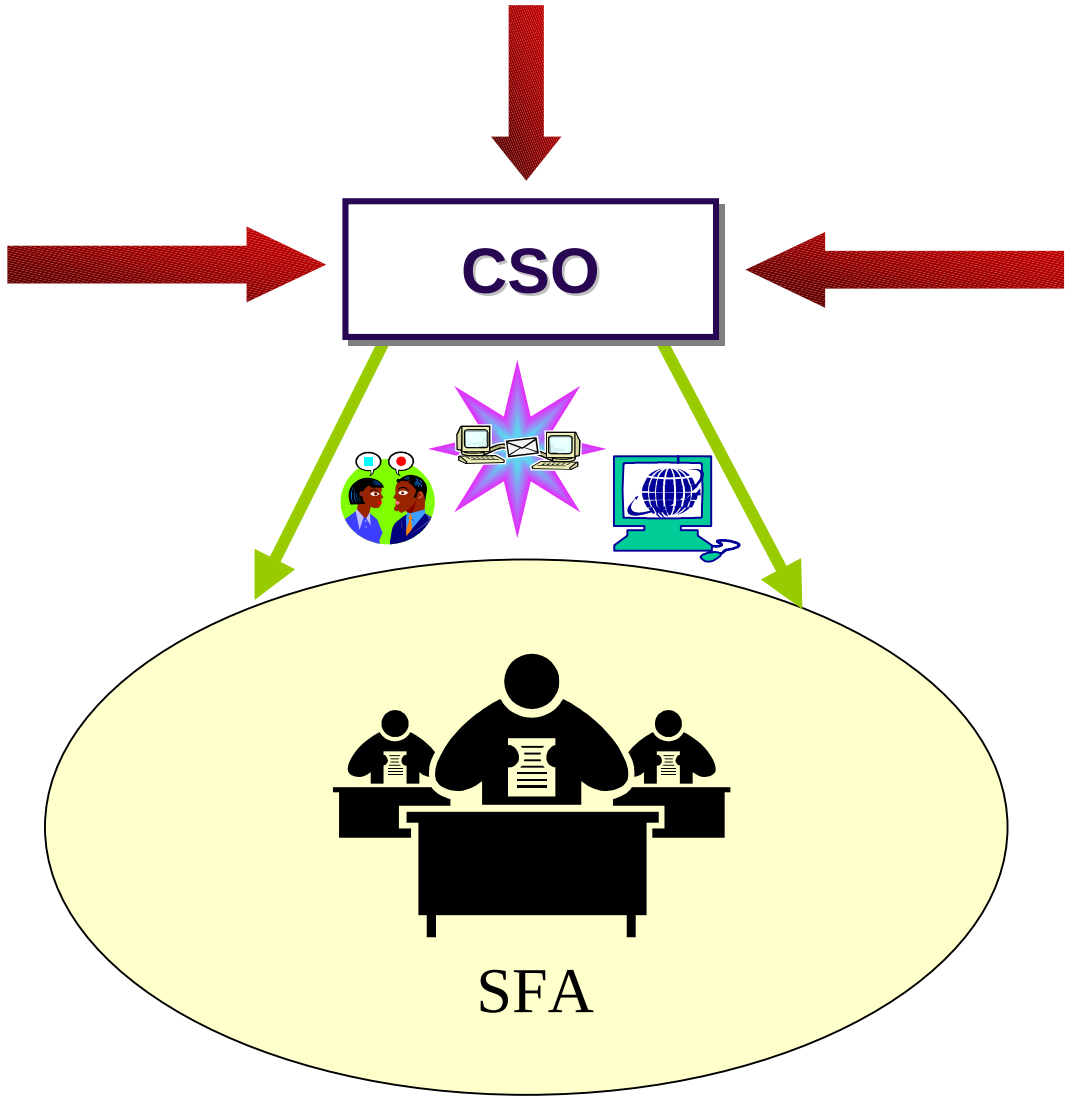
Timeframe

- CSO and security team determine frequency of periodic communications and content determines information demanding immediate release

Area 5: Information Distribution - Scheduled



Area 5: Information Distribution - Immediate



Area 6: Configuration Management

Purpose: To establish security and privacy in SFA's Configuration Management (CM) process, making sure system changes are recorded and adhere to security and privacy policy

Messages

- System configurations and recorded changes
- Impact of changes to system security
- Notifications of implemented configurations

Responsibilities

- CSO staff forwards CM security and privacy guidance to security professionals and maintains an active repository of guidance and past implementations
- Configuration Control Board (CCB) reviews recommended change, considering security ramifications to system, and forwards change to developers
- Vendors and SFA test system changes, then implement the changes and notify SSO upon completion
- SSO forwards implemented configuration report to CSO
- SSO notifies partners, schools and other SFA application SMs of changes that may affect their systems

Communication Methods

- CM security and privacy guidance and repository posted to SFA internet
- CCB meets to discuss and submit recommended system changes
- Requests for and notifications of changes occur on paper/email

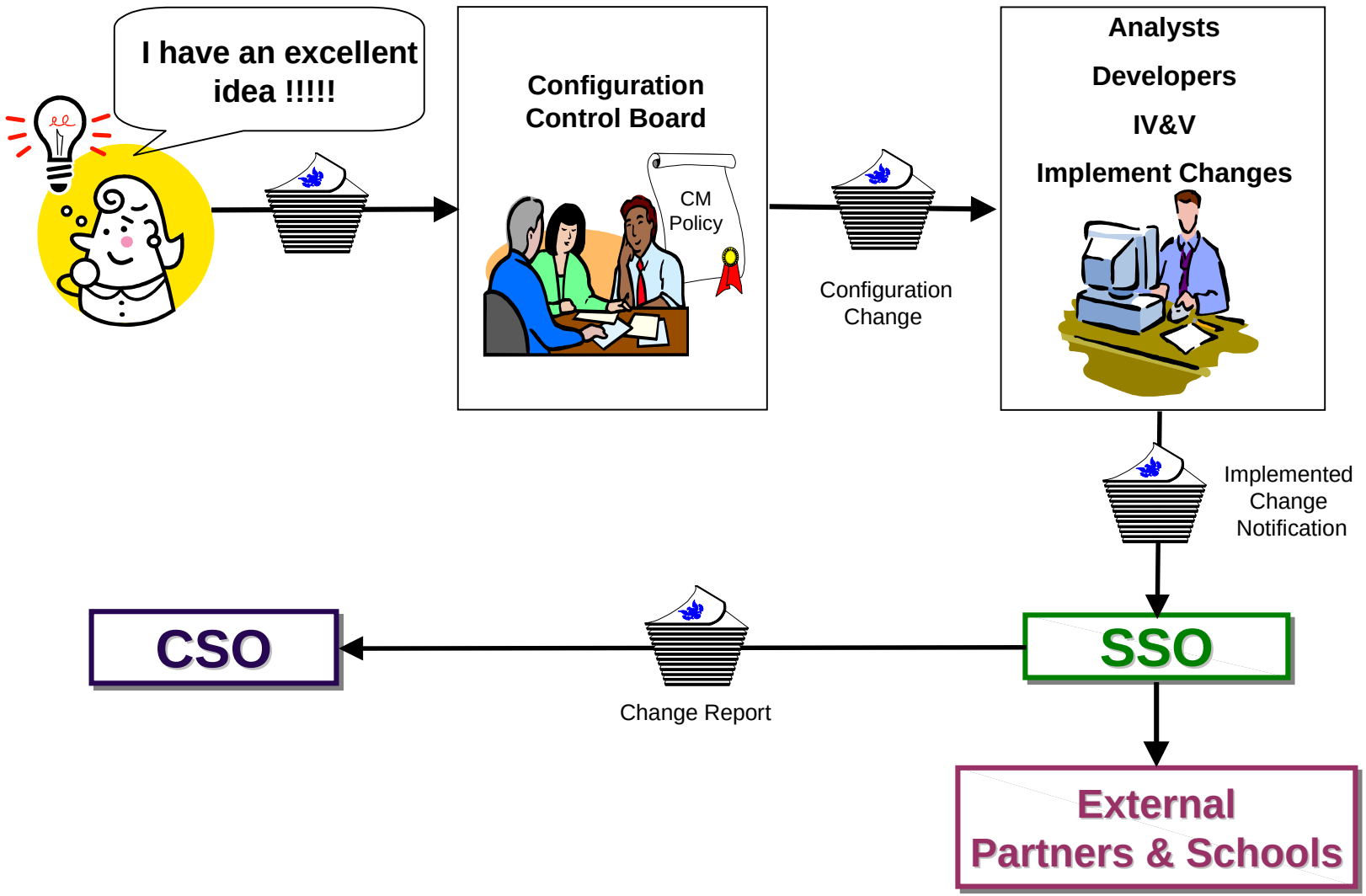
External Communications

- Email to partners, schools and contractors involved in or affected by the changes

Timeframe

- Deadlines specific to the development process that creates, tests and implements the change

Area 6: Configuration Management



Area 7: Procurement

Purpose: To exchange security and privacy guidance for procurement efforts and to establish communication channels between SFA security and system professionals and procurement professionals

Messages

- Security and privacy requirements applicable to procurement process
- Ideas for new hardware, software or services to procure
- Requirements for work to be executed by contractors
- Contract and procurement discussions that lead to delivery of the system or service

Responsibilities

- CSO staff forwards procurement security and privacy guidance to security and procurement professionals
- SM, SSO and systems personnel formulate a need into a requirement, considering impact of security and privacy
- SM forwards final requirements to procurement professionals
- Procurement professionals communicate with SM and SSO about SOW, contract negotiations and tracking of delivered products

Communication Methods

- Procurement guidance posted to SFA intranet and given to SFA acquisition personnel
- Specific procurement efforts and contractual issues passed via email and/or paper to create a traceable log of events
- Meetings and phone calls used for general communications

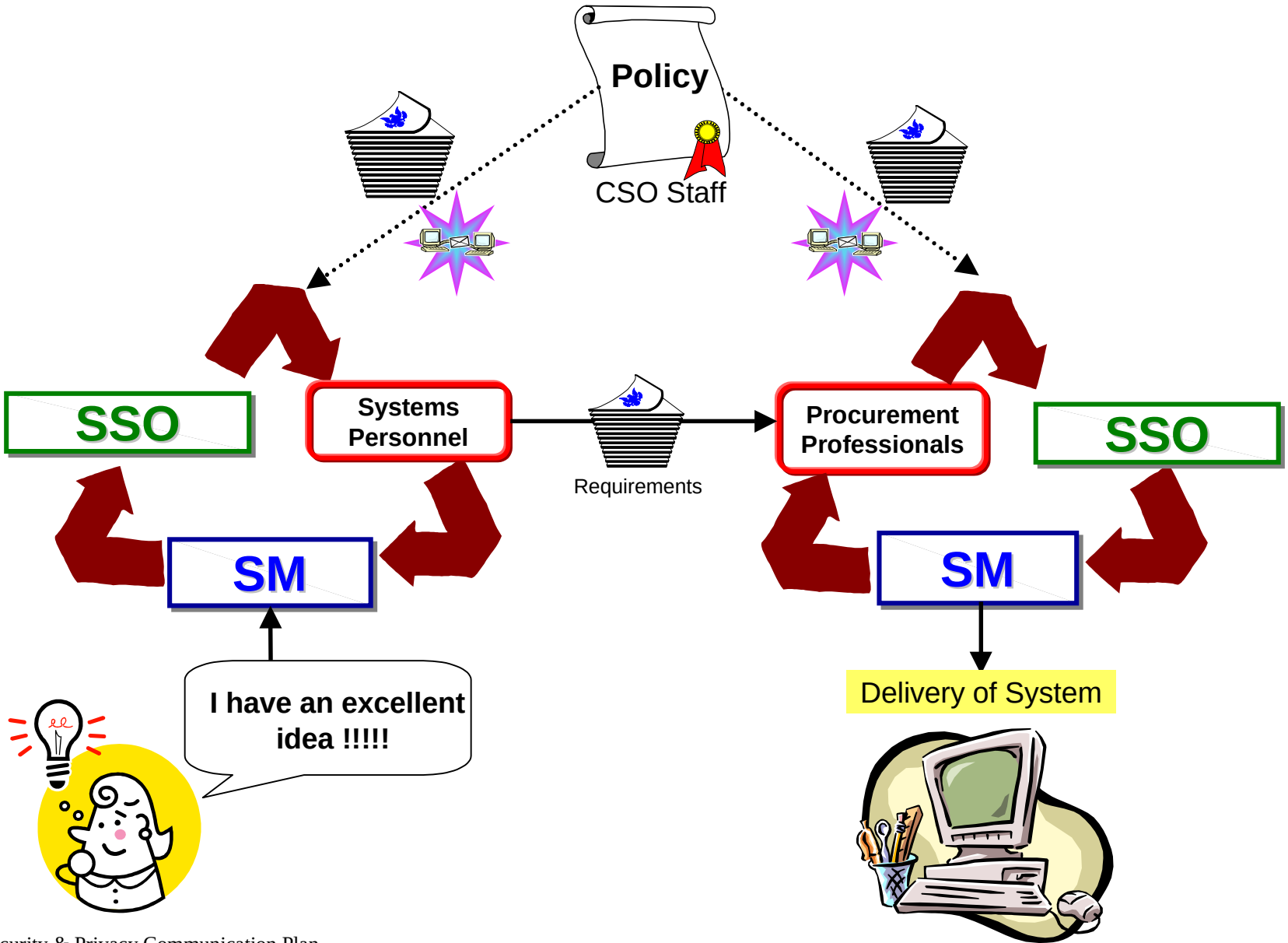
External Communications

- Contracting officer may need to clarify security and privacy issues with vendors

Timeframe

- System delivery determined by contract; security and privacy related issues must be considered before system requirements are finalized

Area 7: Procurement



Area 8: Clearances & Access

Purpose: To exchange personnel clearance information in order to give SFA employees the proper system access to do their jobs

Messages

- Requests for system access
- Requests for background investigations
- Notifications of access approval and termination

Responsibilities

- User submits request for system access and background check materials (as needed) to SFA Personnel Security Officer
- Supervisor signs user request for system access
- SFA Personnel Security Officer checks user clearance status and requests background checks from IG as needed, then informs SSO when user receives the required clearance
- SSO confirms receipt of clearance and informs System Administrator to give user system access
- System Administrator notifies user when his/her access is ready
- SFA HR informs SFA Personnel Security Officer and SSO when a user leaves
- SSO notifies System Administrator to terminate user access and reports actions which warrant revocation of clearances

Communication Methods

- Communications regarding the receipt, status or revocation of clearances must be in writing as original signed documents or signed faxes
- Telephone and email are appropriate for coordination and notification

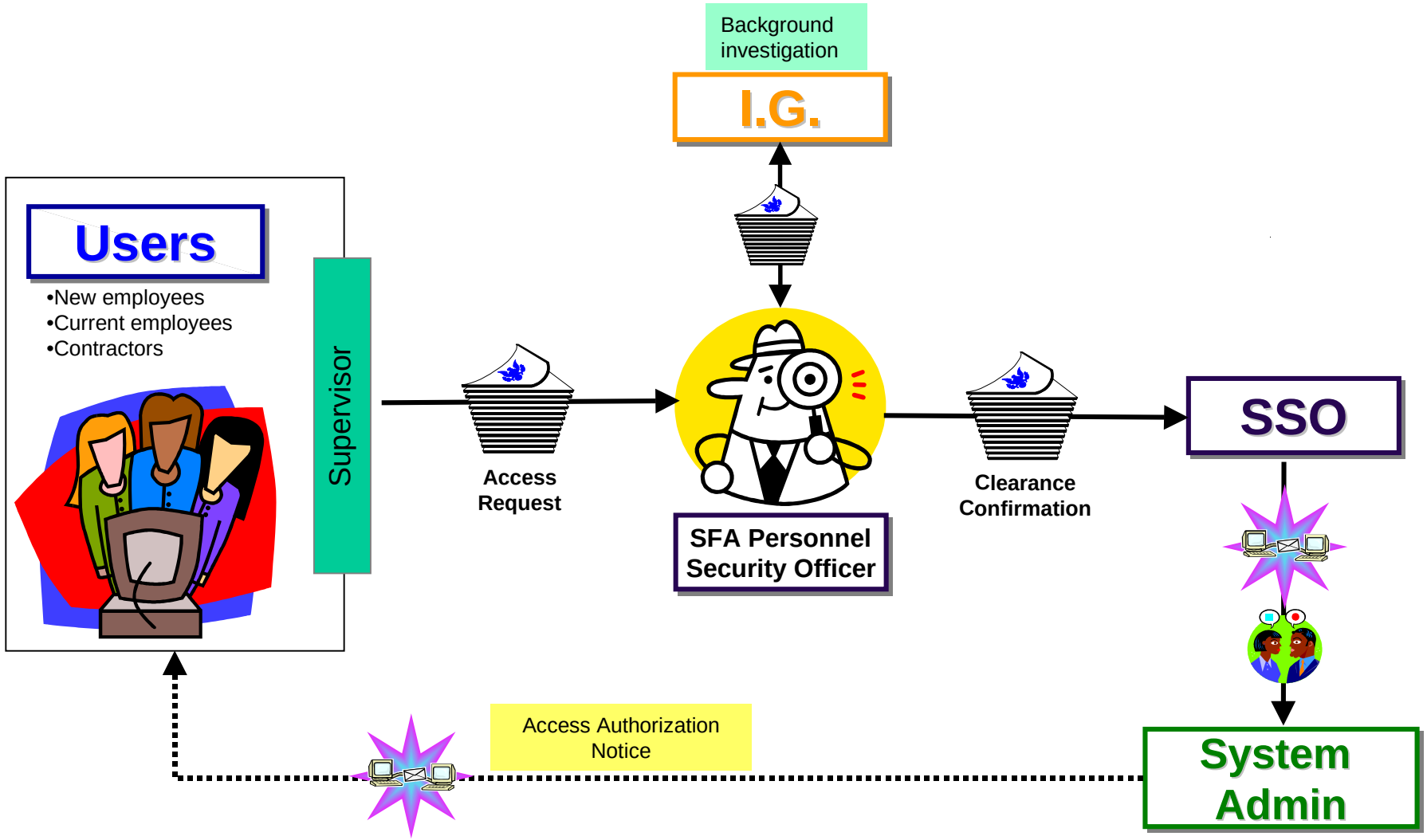
External Communications

- SFA Personnel Security Officer works with the IG to get background investigations performed by OPM

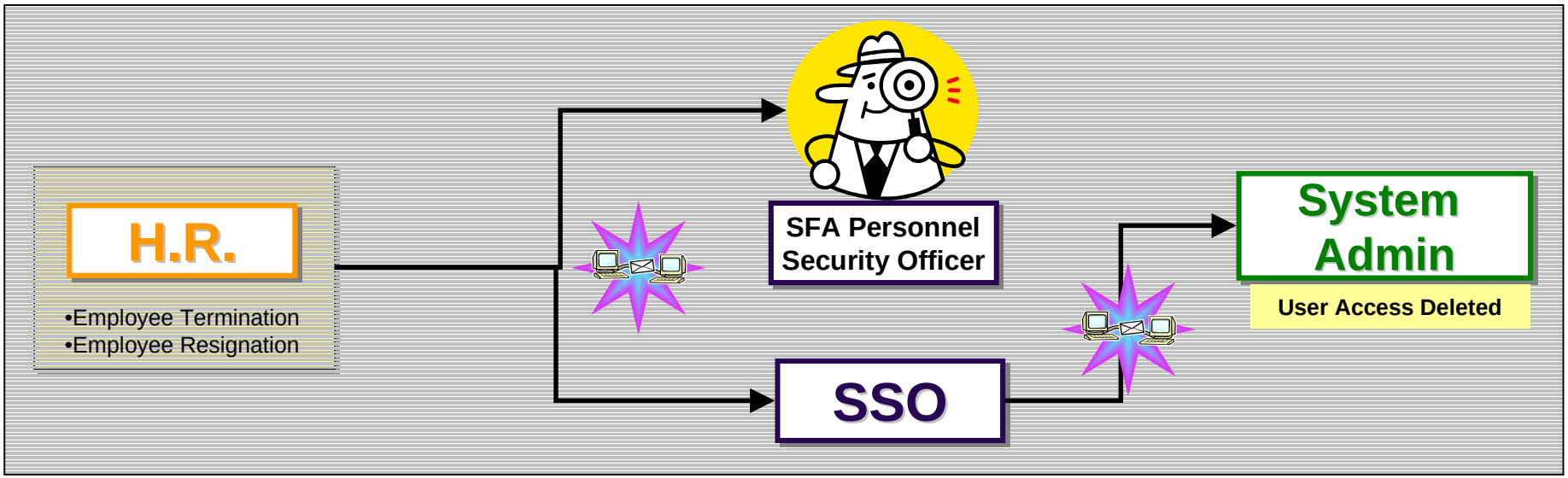
Timeframe

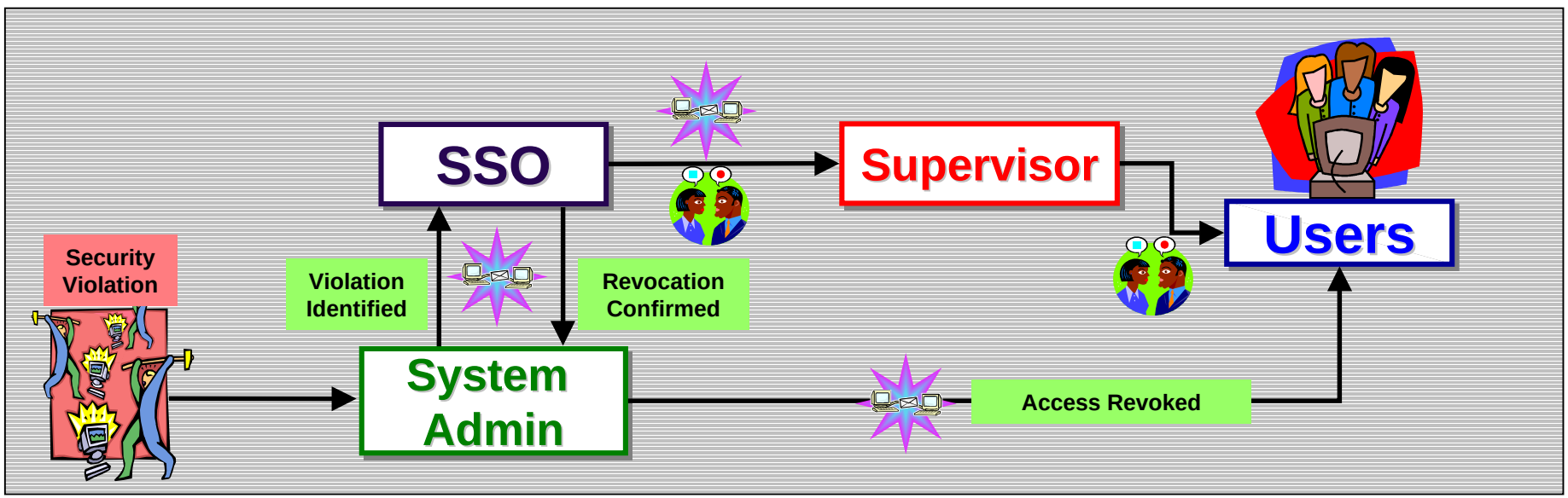
- Specific to needs of the system, program and/or contract

Area 8: Clearances & Access – Getting Access



Area 8: Clearances & Access - Termination





Area 9: Certification and Accreditation (C & A)

Purpose: To exchange information that supports the official validation of SFA systems and security procedures and relates the results back to management

Messages

- Requirements for C & A efforts
- Risk assessment and mitigation plans identifying the residual risk in a system
- C & A validation/findings

Responsibilities

- CSO staff forwards C & A guidance to security professionals and maintains an active repository of guidance and C & A findings for review
- SSOs conduct risk assessments and develop risk mitigation strategies
- SMs review risk assessment and mitigation efforts to successfully certify their system
- SMs incorporate certification findings into an accreditation package and forward to FMs
- FMs complete accreditation findings and forward to CSO

Communication Methods

- C & A guidance and repository are posted to SFA intranet
- C & A packages must be forwarded as hardcopy documents due to the need for approval signatures

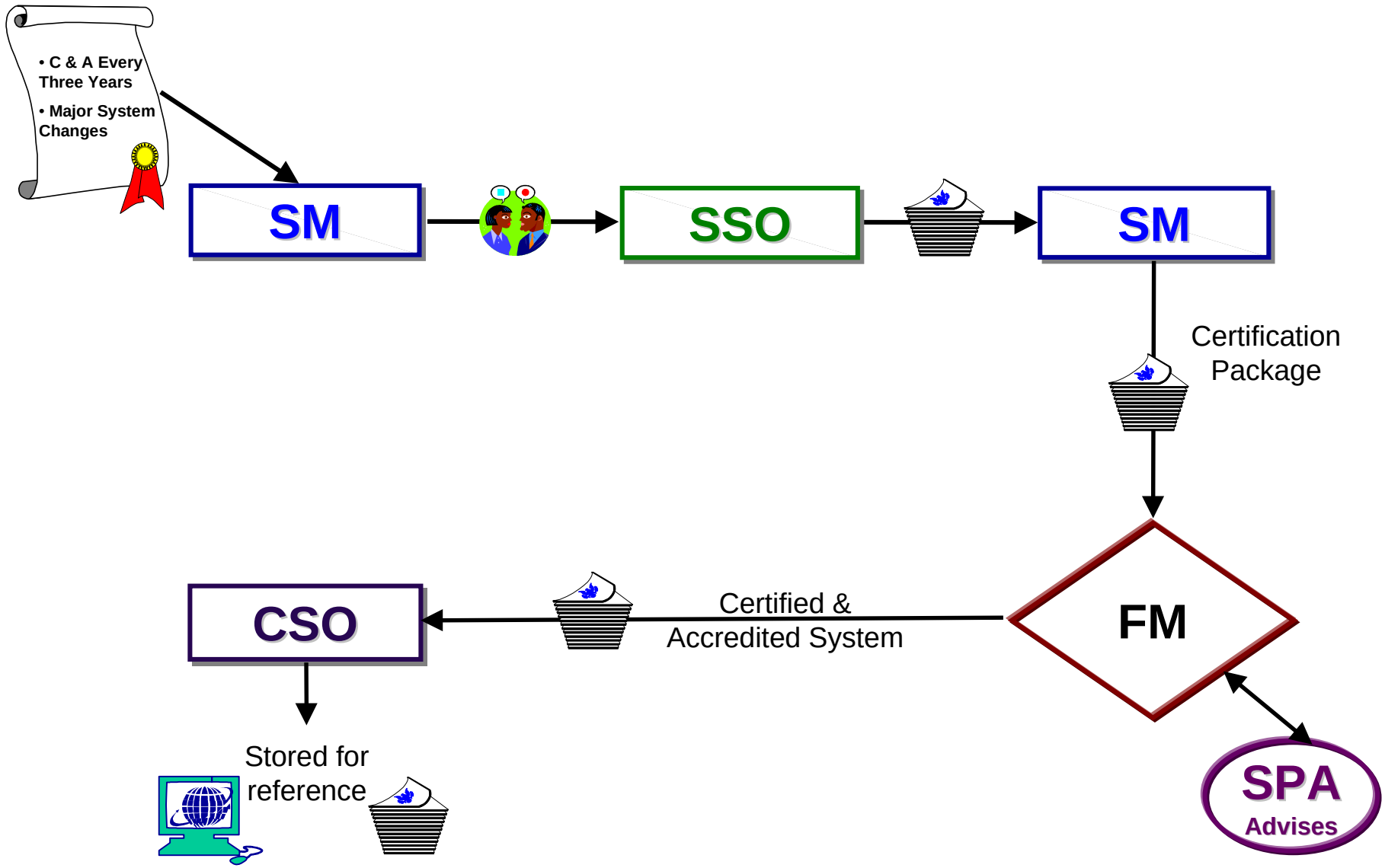
External Communications

- Oversight organizations may require C & A packages for review and may therefore benefit from intranet access

Timeframe

- C & A efforts are required every three years for each system

Area 9: Certification & Accreditation (C & A)



Area 10: Security Professionals Information Exchange

Purpose: To create a forum for the open exchange and resolution of SFA security and privacy issues

Messages

- Policy and guidance directives which help define SFA security and privacy efforts
- Schedules and notices of working groups
- Outcomes from the working groups

Responsibilities

- CSO establishes all SFA-wide security and privacy working groups, as well as appoints SFA representatives to external working groups (e.g., Department of Education)
- CSO staff schedules and announces working group sessions, develops agendas, maintains meeting minutes and tracks action items
- Working group members present materials pertinent to the agenda items, and act as the conduit for items specific to their systems

Communication Methods

- Working group schedules, agendas, minutes and action items are distributed via email
- Actual sessions involve facilitated discussions structured around an agenda and assigned action items
- Contact with external organizations is conducted by the most effective method to reach each organization

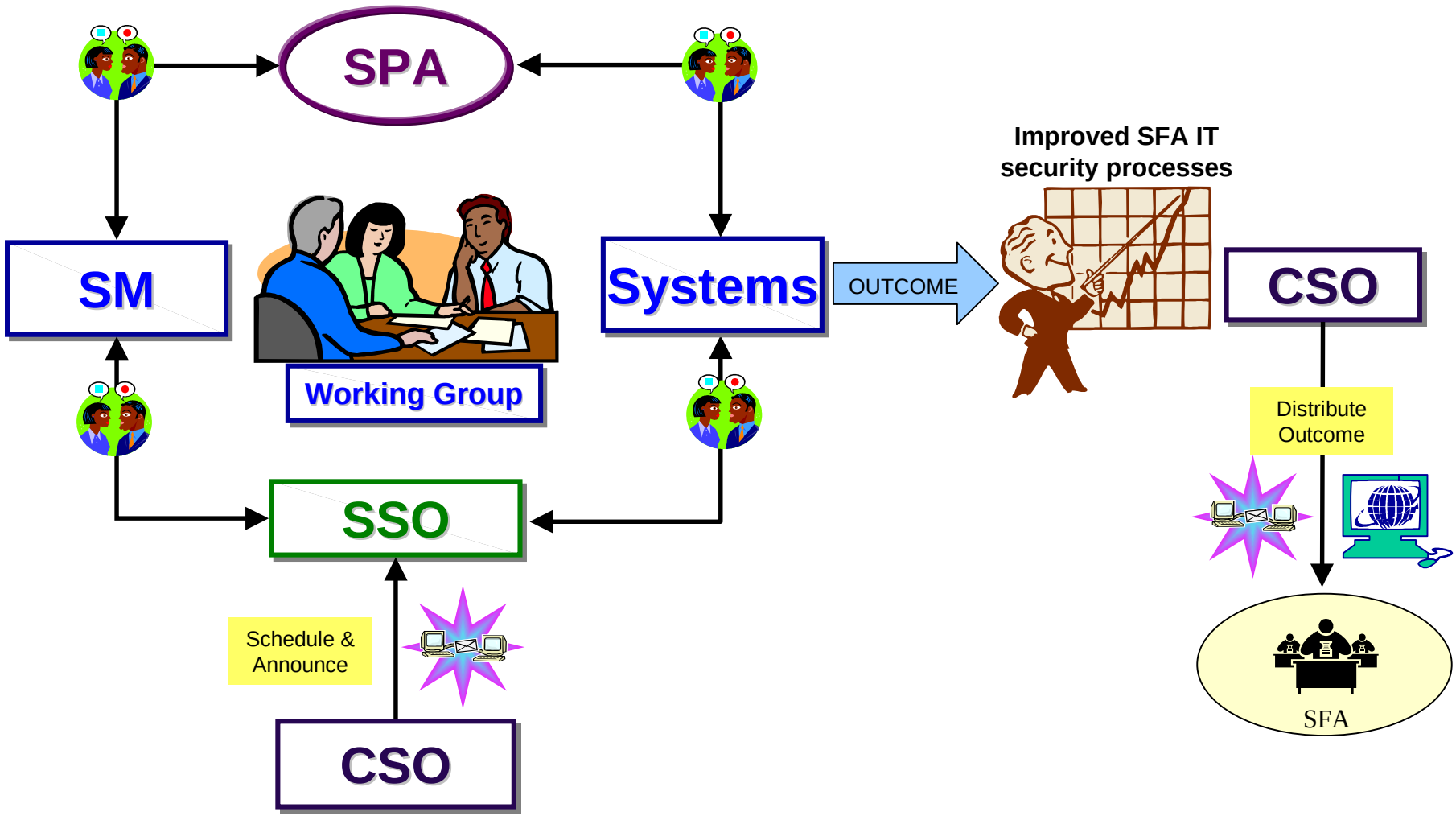
External Communications

- Some working groups may be hosted by outside organizations (e.g., FedCIRC) or require the participation of partners, associations and schools

Timeframe

- Determine by type of working group: standing body that meets periodically for a specific function or ad hoc group created to address a specific short term need
- Notify working group members in time for them to plan to attend

Area 10: Security Professionals Information Exchange



Area 11: User Questions & Answers

Purpose: To provide SFA system users and customers with answers to security and privacy questions and problems

Messages

- Security and privacy questions and problems about SFA systems
- Answers to Frequently Asked Questions (FAQs)
- Points of Contact (POCs) for questions by topic area and general questions
- Responses to requests for assistance

Responsibilities

- Users know to seek help with security and privacy problems
- CSO staff develops FAQ and POC lists and directs questions they receive to appropriate functional areas
- Help desks answer questions directly or forward requests for assistance to the appropriate functional areas
- Functional areas responding to requests answer the user directly

Communication Methods

- Access to FAQs and POCs via the SFA intranet and extranet; help material on SFA internet site supports customers
- Requests for assistance submitted via email or phone; if email, a confirmation email will be returned to the requester
- Updates and final answers provided via email, phone, or in-person

External Communications

- Answers given to questions from customers, partners and contractors

Timeframe

- Determined by priority of user's problem and whether solution requires research

Area 11: User Questions & Answers